



[6450-01-P]

## DEPARTMENT OF ENERGY

### Energy Sector Framework Implementation Guidance

AGENCY: Department of Energy.

ACTION: Request for Public Comment.

SUMMARY: The Department of Energy (DOE) invites public comment on DOE's draft document *Energy Sector Cybersecurity Framework Implementation Guidance* (Guidance). The document is available for a 30 day comment period at <http://energy.gov/node/942856>.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Comments to be submitted electronically must be submitted through the Email address [Cyber.Framework@hq.doe.gov](mailto:Cyber.Framework@hq.doe.gov) using the submission form at <http://energy.gov/node/942856>. Written comments may be submitted to Akhlesh Kaushiva, Program Manager, Office of Electricity Delivery and Energy Reliability, U. S. Department of Energy, 1000 Independence Avenue, SW, Washington, D.C. 20585.

FOR FURTHER INFORMATION CONTACT: Requests for additional information should be directed to Akhlesh Kaushiva, Program Manager, Office of Electricity Delivery and Energy Reliability, U. S. Department of Energy, 1000 Independence Avenue, SW, Washington, D.C. 20585 at [Cyber.Framework@hq.doe.gov](mailto:Cyber.Framework@hq.doe.gov).

SUPPLEMENTARY INFORMATION: Since the release of the Cybersecurity Framework by the National Institute of Standards and Technology (NIST) on February 12, 2014, DOE has collaborated with private sector stakeholders through the Electricity Subsector Coordinating Council (ESCC) and the Oil & Natural Gas Subsector Coordinating Council (ONG SCC) forums for the development of the draft Guidance. The DOE, through a notice published in Federal Register on June 20, 2014, requested energy sector organizations to participate in the ESCC and ONG SCC forums. The DOE has also been coordinating with other Sector Specific Agency (SSA) representatives and interested government stakeholders for the development of the draft Guidance and to address cross-sector overlaps. The primary goal of the document is to help energy sector stakeholders develop or align existing cybersecurity risk management programs to meet the objectives of the Cybersecurity Framework. The document will also help energy sector organizations effectively demonstrate and communicate their cybersecurity risk management approach and use of the Framework to both internal and external stakeholders.

Authority:

Section 8 (b) Executive Order 13636 “Improving Critical Infrastructure Cybersecurity”

Issued at Washington, DC on September 8, 2014.

---

Patricia A. Hoffman,  
Assistant Secretary,  
Electricity Delivery and Energy Reliability.

[FR Doc. 2014-21840 Filed 09/11/2014 at 8:45 am; Publication Date: 09/12/2014]